IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE MICHAELS STORES PIN PAD LITIGATION	Case No. 1:11-cv-03350
- -	Honorable Charles P. Kocoras
This Documents Relates to All Actions	

PLAINTIFFS' MEMORANDUM OF LAW
IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

Dated: September 9, 2011

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

I. INTRODUCTION

Plaintiffs Mary Allen, Kelly M. Maucieri, Brandi Ramundo, and Adrianna Sierra (collectively, "Plaintiffs"), by their undersigned counsel, respond as follows in opposition to Defendant Michaels Stores, Inc.'s ("Michaels," the "Company," or "Defendant") Motion to Dismiss (Dkt. No. 34) and Memorandum of Law in Support (Dkt. No. 36, hereinafter "Def. Mem."). For the reasons set forth below, Plaintiffs respectfully submit that Michaels' motion to dismiss should be denied in its entirety.

II. STATEMENT OF FACTS

Plaintiffs bring this action individually and on behalf of all consumers whose identity and personal financial information was stolen from Michaels stores across the United States ("Class"). *See generally* Plaintiffs' Consolidated Amended Class Action Complaint ("CAC" or "Complaint"). Michaels failed to provide basic security measures, which allowed thieves to install and operate hacked PIN pad payment terminals in ***eighty stores*** in at least 20 states, without detection, for an extended period of time. *Id*. at ¶¶ 4, 45. To date, more than 1,000 individuals have had money stolen from their bank accounts via Automatic Teller Machine withdrawals on the West Coast after swiping their debit or credit cards at Michaels. *Id.* at ¶ 45.

Adding insult to injury, Michaels also failed to alert Class members in a timely manner to this massive security breach. *Id.* at ¶ 60. Michaels' failure to provide prompt and adequate notice of the breach has prevented Class members from protecting their personal information from further abuse. *Id.* at ¶ 9.

A. Michaels' Massive PIN Pad Security Breach

Michaels failed to implement basic security measures to protect Class members' personal financial information on their credit and debit cards in an effort to avoid the expense of complying with best practices and industry standards concerning PIN pad security as well as

Michaels' contractual obligations to card issuers. CAC at ¶ 7. Particularly, Visa contractually requires all merchants who accept their credit and debit cards, including Michaels, to comply with various PIN security standards. *Id.* at ¶ 26. These standards include the "Visa Global Mandate," which requires that all PIN pad terminals in use after July 1, 2010 comply with certain enhanced security protections making them tamper resistant. *Id.* at ¶¶ 26, 29, 32. The payment card industry has also promulgated standard procedures to prevent PIN pad tampering of older, outdated devices. *Id.* at ¶¶ 39-40. Indeed, PIN pad terminal swapping is easily prevented by using modern PIN pad devices which immediately shut down when tampered with. *Id.* at ¶ 43.

Michaels, however, (1) failed to enact basic security measures to detect or prevent PIN pad tampering; (2) failed to follow industry standards for PIN pad and store security; and (3) failed to use tamper resistant PIN pads in all of its stores. *Id.* at ¶ 51, 79, 93.[1]

B. Michaels Compromises Class Members' Personal Financial Information

Between February 8, 2011 and May 6, 2011, skimmers installed tampered PIN pad terminals in eighty Michaels stores across at least twenty states. *Id.* at ¶ 45.[2] In late April 2011, Class members in the Chicago area began to report unauthorized withdrawals from ATM machines in California after using their debit cards at Michaels stores. *Id.* at ¶ 48. Shortly thereafter, other Class members across the United States suffered unauthorized ATM withdrawals from their bank accounts. *Id.* at ¶ 50. Class members whose personal financial information was compromised remain vulnerable to further identity theft. *Id.* at ¶ 49-50.

[1] That "Michaels was authorized by Visa to accept Visa credit and debit cards for the payment of personal goods" as alleged in the complaint, *see* CAC ¶ 27, 30, 33, is unfairly construed by Michaels to support their contention that they were in full compliance with their contractual obligations. *See* Def. Mem. at 17-18. But Michaels' construction must be rejected, as Plaintiffs clearly and directly allege that Michaels was not in compliance Visa's requirements as well as industry standards. See CAC ¶¶ 51-53, 93, 107, 123.

[2] The data breach may have occurred as early as December 2010 and the number of affected stores is even larger than Michaels has reported. *Id.* at ¶ 46.

C. Michaels Fails to Provide Timely Notice of the Data Breach

On May 4, 2011, almost three months after the first data breach occurred, Michaels issued a limited report on its Facebook webpage, in which it downplayed the risk and severity of the situation by representing that PIN pad tampering ***may*** have occurred in its Chicago area stores. *Id.* at ¶ 56. In fact, Michaels must have been aware at the time that many of its customers had money stolen from accounts linked to debit cards that were used in Michaels stores, because one day earlier, on May 3, 2011, law enforcement agencies were already informing victimized Michaels customers that the thefts had been traced to their use of a debit card at Michaels stores. *Id.* at ¶ 18.[3]

On May 5, 2011, Michaels emailed a Customer Security Alert to a small subset of its customers (the "Email Alert"). The Email Alert misled Michaels customers about the severity of the data breach. Michaels represented that "it ***may have been*** a victim of PIN pad tampering in the Chicago area and that customer credit and debit card information ***may have been*** compromised." (emphasis supplied). *Id.* at ¶ 56. Subsequent updates appeared only in the "Customer Notices" page of Michaels' website. *Id*. at ¶ 56. In one such update, the Company greatly expanded its recognition of the scope of the breach to include approximately eighty stores in twenty states. Nevertheless, the true scope of the data breach is far greater than what Michaels has represented in its disclosures to date. *Id*. at ¶ 56. Indeed, right now, thousands of Class members who used their debit and credit cards at affected Michaels stores, during a period when Michaels knows that customer data was stolen, are unaware of Michaels' security breach and their own dramatically increased risk of becoming victims of identity theft. *Id*. at ¶ 60.

[3] When Michaels *actually* learned of the data breach is a material issue of fact that cannot be resolved on a motion to dismiss. Plaintiffs have not pled, and do not concede, that Michaels learned of the breach on May 4, 2011; rather Plaintiffs have alleged that Michaels *announced* or *reported* that it learned of the breach on May 4, 2011. CAC ¶¶ 2, 45, 56-57; *cf.* Def. Mem. at 2, 19-20.

III. ARGUMENT

A. Legal Standard

The Court must accept Plaintiffs' well-pleaded allegations of fact as true, and draw any inferences in Plaintiffs' favor. *Disability Rights Wisc., Inc. v. Walworth County Bd. Of Supervisors*, 522 F.3d 796, 799 (7th Cir. 2008); *see also Rowe v. Unicare Life & Health Ins. Co.*, No. 09-C2286, 2010 WL 86391, at *1-2, , 2010 U.S. Dist. LEXIS 1576, at *3-4 (N.D. Ill. Jan. 5, 2010) (Hibbler, J.) ("Motions to dismiss test the sufficiency, not the merits, of the case. *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). To survive a motion to dismiss, a plaintiff must 'provide the grounds of his entitlement to relief' by alleging 'enough to raise a right to relief above the speculative level.' *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).") (brackets omitted).

B. Plaintiffs Allege Actual Injuries And Compensable Damages

Notwithstanding Defendant's contentions to the contrary, Plaintiffs sufficiently plead damages that establish their concrete and compensable right to relief.

First, Plaintiffs allege they suffered and continue to suffer compensable damages, including lost money, caused by Michaels' misconduct. *See, e.g.*, CAC ¶¶ 16-19, 101 ("Plaintiffs and the other Illinois Subclass members *have suffered injury in fact and actual damages including lost money* . . . .") (emphasis supplied); CAC ¶ 125 ("Plaintiffs and the other Class members *suffered and will continue to suffer damages including, . . . loss of money* . . . .") (emphasis supplied). Specifically, Plaintiffs allege they and the other Class members were damaged in that, as a result of Michaels' lax security, which enabled skimmers to obtain their personal financial information, they sustained monetary losses arising from unauthorized bank

account withdrawals and/or related bank fees charged to Plaintiffs' accounts.[4] *See* CAC ¶¶ 16-19.[5]

Second, Plaintiffs also allege that they suffered and continue to suffer compensable damages from lost property as a result of Michaels' misconduct. *See, e.g.*, CAC ¶¶ 101, 125. Specifically, Plaintiffs allege lost property as a result of Michaels' failure to employ adequate security measures. *See* CAC ¶¶ 16-19.[6] To make in-store purchases at Michaels with their debit or credit cards, Plaintiffs were required to provide their cards' magnetic strip data and their PINs (for debit cards only) for payment verification. *See* CAC ¶ 120. By accepting Plaintiffs' and other Class members' non-public information, Michaels was obligated to reasonably safeguard that information. *See id.* ¶¶ 106, 121; *see also Richardson v. DSW, Inc.*, Case No. 05 C 4599, 2005 U.S. Dist. LEXIS 26750, at *10 (N.D. Ill. Nov. 3, 2005) ("*Richardson I*") (noting "it would

[4] Michaels infers Plaintiffs did not have to pay any unauthorized charges, or that the unauthorized charges "remain unreimbursed." Def.'s Mem. at 10. Such an inference, however, is not supported by the Complaint's actual allegations. *See, e.g.*, CAC ¶ 125.

[5] Other courts have upheld similar damages claims in analogous cases. *See, e.g.*, *Stollenwerk, et al. v. Tri-West Health Care Alliance*, 254 F. App'x. 664, 667-68 (9th Cir. 2007) (reversing summary judgment as to negligence claim, holding that plaintiff established causal connection between wrongful conduct and the alleged damages); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1111-14 (N.D. Cal. 2010) (on a motion for judgment on the pleadings, finding sufficient allegations of injury based on AOL's public disclosure of plaintiffs' confidential member information under particularized damages requirements for specific causes of action); *Jones v. Commerce Bancorp, Inc.*, No. 06 Civ. 835, 2006 U.S. Dist. LEXIS 32067, at *4-14 (S.D.N.Y. May 23, 2006) (denying motion to dismiss breach of fiduciary duty, negligence, and breach of contract claims notwithstanding plaintiff's concession that defendant credited stolen funds back to her account); *Daly v. Metropolitan Life Ins. Co.*, 782 N.Y.S.2d 530, 532, 535-36 (N.Y. Sup. Ct. 2004) (denying motion for summary judgment on negligence claim where janitor who cleaned defendant's offices illegally accessed plaintiff's confidential personal information and used same to fraudulently establish and use credit card accounts, and concluding that the damage analysis "is a question of fact for a jury to decide.").

[6] By failing to challenge Plaintiffs' property damage allegations in its Motion to Dismiss, Michaels has waived its opposition to those claims. *See, e.g.*, *Cent. States, Southeast & Southwest Areas Pension Fund v. C. & V. Leasing, Inc.*, Case No. 09 C 2871, 2010 U.S. Dist. LEXIS 79532, at *14, n.3 (N.D. Ill. July 30, 2010) ("C&V advances no argument regarding timeliness, and indeed has waived such an argument by [failing to raise it]."); *see also Guinto v. Exelon Generation Co., LLC*, 341 Fed. Appx. 240, 248, n.3 (7th Cir. 2009) ("We note that Guinto has not challenged the district court's analysis under the direct method. We therefore consider this argument waived. . . .").

be possible to find that DSW [a retailer] not only offered to accept certain forms of non-cash payment in exchange for shoes but also offered to take reasonable measures to keep this information secure."); *Daly*, 782 N.Y.S. 2d at 535 ("[T]his court is convinced that Met Life had a duty to protect the confidential personal information provided by plaintiffs.").

Plaintiffs have a property right in the private information that was compromised and lost by Michaels' failure to provide adequate security. *See generally People v. Kozlowski*, 96 Cal. App. 4th 853, 866-67 (2002) (finding that a person's ATM PIN code constitutes valuable intangible property in the context of extortion). Michaels breached its obligations to Plaintiffs and the other Class members by failing to take reasonable measures to safeguard their property. *See* CAC ¶ 123. As a result, Plaintiffs suffered and will continue to suffer damages because of Defendant's failure to secure their private information, including "loss of their financial information." *See id.* at ¶ 125; *Doe 1 v. AOL LLC*, 719 F. Supp. 2d at 1111-12 (denying motion for judgment on the pleadings based on finding that plaintiffs were injured by public disclosure of their confidential information in violation of defendant's obligation to safeguard same).

Moreover, Plaintiffs' personal financial information has value that was lost due to Michaels' wrongful conduct. It is indisputable that such personal data has tangible value and that companies pay substantial amounts of money for such data. Indeed, a new category of business, so-called "privacy brokers," have created a market for the purchase and sale of individuals' personal information. *See* WSJ Article, *Web's Hot New Commodity: Privacy*, Feb. 28, 2011 ("Allow Ltd. . . . offers to sell people's personal information on their behalf, and give them 70% of the sale). Accordingly, Plaintiffs' private personal information has real, concrete value, the loss of which constitutes actual harm.

Third, Plaintiffs also allege compensable harm arising from the costs associated with identity theft and the increased risk of identity theft caused by Michaels' wrongful conduct. Plaintiffs allege numerous instances of actual identity theft that require credit monitoring services now and in the future. *See* CAC ¶¶ 110, 117, 125. Even where a defendant merely exposes an individual's personal data and the plaintiff does not allege that anyone actually accessed the exposed information, Illinois law allows recovery of damages incurred to mitigate the increased risk of future harm. *See Rowe*, 2010 U.S. Dist. LEXIS 1576, at *21-22 ("[G]iven the fact that Illinois courts do allow plaintiffs to recover damages based on the increased risk of future harm, it is appropriate to allow present damages that are meant to mitigate that increased risk. . . . federal courts have accepted the increased risk of future harm as an injury and allowed for the recovery of future damages.").[7]

In opposing Plaintiffs' damage allegations, Michaels relies upon numerous distinguishable cases. As an initial matter, Plaintiffs' damages allegations include actual misuse of their confidential information and actual instances of identity theft resulting in lost money and property. *See* CAC ¶¶ 16-19. As a result, this case starkly contrasts with other data breach cases where plaintiffs alleged damages based merely upon the availability or breach of their confidential information and attendant increased potential for risk of identity theft without any allegations of actual misuse.[8]

[7] Defendant cites *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007), for the proposition that time and money expended to detect or prevent identity theft is not a compensable injury. *See* Def. Mem. at 11. However, in *Rowe*, this District held that *Pisciotta* offered little guidance because it was decided under Indiana law which was contrary to Illinois law allowing recovery of damages based on the increased risk of future harm. 2010 WL 86391, at *7, 2010 U.S. Dist. LEXIS 1576 at 20-21.

[8] *See Cooney v. Chicago Public Schools*, 943 N.E.2d 23, 27 (Ill. App. Ct 1st Dist. 2010) (no allegation of actual misuse of personal information); *Katz v. Pershing, LLC*, No. 10-12227-RGS, 2011 WL 1113198, at *1 (D. Mass. Mar. 28, 2011) (plaintiff failed to allege that any of her nonpublic personal information had been lost, stolen, disclosed, or accessed by an unauthorized person); *Zeldman v. Pershing LLC*, No. 1:09-cv-22609 (JAL), Order at 4 (S.D. Fla. Aug. 20, 2010) (same in unpublished opinion); *McLoughlin v.*

Defendants also cite a series of summary judgment cases where laptops or hard drives containing personal information were stolen. *See* Def. Mem. at 10 fn 6. In each of these cases, however, the courts dismissed the plaintiffs' claims only after those plaintiffs failed to show that the thieves stole the storage device with the intent to misuse the information or that any information was actually misused.[9] In contrast, Plaintiffs here can show cognizable injury because Michaels exposed their personal information to third parties without password or other protection, the skimmers who stole the data were motivated by a desire to access the data for personal gain, and the skimmers actually did access the data and steal money from Plaintiffs and other Class members.

People's United Bank, Inc., No. 3:08-cv-00944 (VLB), 2009 WL 2843269, at *4 (D. Conn. Aug. 31, 2009) (no allegation that plaintiffs' information was misused); *Shafran v. Harley-Davidson, Inc.*, No. 07 Civ. 01365 (GBD), 2008 WL 763177, at *1 (S.D.N.Y. Mar. 20, 2008) (same); *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 796 (M.D. La. Nov. 7, 2007) (same); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 688 (S.D. Ohio 2006) (same); *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d 775, 777 (W.D. Mich. 2006) (same); *see also Frye v. L'Oreal USA, Inc.*, 583 F. Supp. 2d 954, 958 (N.D. Ill. 2008) (dismissing case where "there is no allegation that the presence of lead in the lipstick had any observable economic consequences.")

[9] *See Resnick v. AvMed, Inc.*, 2011 WL 1303217, at *1 (S.D. Fla. Apr. 5, 2011) (no allegation that "theft of several laptops from Defendant's corporate headquarters" resulted in actual misuse of personal employee information); *Ruiz v. Gap, Inc.*, 380 Fed. Appx. 689, 690 (9th Cir. Cal. 2010); *Kahle v. Litton Loan Servicing LP*, 486 F. Supp. 2d 705 (S.D. Ohio 2007) ("Plaintiff has admitted, that to her knowledge, no unauthorized use of her personal information has occurred. She has not been a victim of identity fraud since the theft, which occurred 20 months ago. . . Thus, any injury of Plaintiff is purely speculative."); *Krottner v. Starbucks Corp.*, 2009 WL 7382290, 2009 U.S. Dist. LEXIS 130634, at *27-28 (W.D. Wash. Aug. 14, 2009) (dismissing after laptop containing employee personal information where there was no proof of information misuse); *Guin v. Brazos Higher Educ. Servs. Corp.*, 05-668, 2006 U.S. Dist. LEXIS 4846 (Feb. 7, 2006) (citing plaintiff's failure to establish a cognizable injury because there was no evidence that plaintiff's personal information was accessed by the thieves, plaintiff experienced no identity theft or other fraud as a result of the stolen information and no one else whose information was stolen had been the subject of identity theft to the defendant's knowledge); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 282 (S.D.N.Y. 2008) (same, and also noting "factors giving rise to a demonstrable basis for a serious concern over misuse may include evidence of the following: (1) the lack of any password-protection for use of the computer such that an unsophisticated user could boot the computer and immediately access the file; (2) that the person stealing the hard drive was motivated by a desire to access the data and had the capabilities to do so; or (3) actual access or misuse of information of the plaintiff or another person whose data was stored on the same hard drive."); *see also Hammond v. The Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, 2010 U.S. Dist. LEXIS 71996, at *17-21 (S.D.N.Y June 25, 2010) (dismissing on summary judgment after plaintiffs could not link any misuse of personal information to defendant's loss of backup tapes containing personal information).

Finally, to the extent that Michaels relies on Judge Hornby's opinion in *In re Hannaford Bros. Data Sec. Breach Litig.*, 613 F. Supp. 2d 108 (D. Maine 2009) to support their lack of injury argument, Michaels overreaches. Judge Hornby specifically limited his opinion to then-current Maine law, concluding that "under current Maine law, consumers whose payment data are stolen can recover against the merchant only if the merchant's negligence caused a direct loss to the consumer's account." *In re Hannaford*, 613 F. Supp. 2d at 136. As discussed above, however, Illinois law allows recovery of indirect damages incurred to mitigate the increased risk of future harm. *See Rowe* 2010 U.S. Dist. LEXIS 1576, at *21-22.

In sum, Plaintiffs sufficiently allege actual and compensable injuries.

C. Plaintiffs Sufficiently Plead Their ICFA Claim

Plaintiffs allege sufficient facts to state a claim under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* ("ICFA"). Plaintiffs allege that Michaels' gross failure to maintain reasonable and adequate data security, thereby exposing Plaintiffs' sensitive personal and financial information to criminals was an unfair and deceptive practice in violation of the ICFA. CAC ¶¶ 4, 6, 51-53, 90-98. Plaintiffs further allege that Michaels' immediate and ongoing failures to provide prompt notice of the security breach constitute ICFA violations as well. CAC ¶¶ 46-47, 54-61, 99-100.

The IFCA "is a regulatory and remedial statute intended to protect consumers, borrowers, and business persons against fraud, unfair methods of competition, and other unfair and deceptive business practices" and "is to be liberally construed to effectuate its purpose." *Robinson v. Toyota Motor Credit Corp.*, 775 N.E.2d 951, 960 (Ill. 2002) (citing *Cripe v. Leiter*, 703 N.E.2d 100 (Ill. 1998)).[10] As numerous courts have noted, "[t]he terms of the Act are

[10] Michaels' contention that the ICFA cannot apply because Michaels' inadequate security led to security breaches in more than twenty states is legally unsupportable. Def. Mem. at 12 n.9. Neither of the cases

incapable of precise definition; accordingly, whether a given set of circumstances is unfair or deceptive must be determined on a case-by-case basis." *Falcon Assocs. v. Cox,* 699 N.E.2d 203, 210 (Ill. App. Ct. 5th Dist. 1998) (citing *People ex rel. Fahner v. Walsh*, 461 N.E.2d 78, 81 (Ill. 1984)).

To state a violation of the ICFA, a plaintiff must allege: "(1) an unfair or deceptive act or practice by the defendant; (2) the defendant's intent that plaintiff rely on the deception; and (3) the occurrence of the deception in the course of conduct involving trade or commerce." *Parks v. Wells Fargo Home Mortgage, Inc.*, 398 F.3d 937, 942 (7th Cir. 2005). Further, the defendant's unfair or deceptive practice must be intentional and inure to the defendant's benefit. *Id*. Proximate causation is also an element of all private causes of action under the ICFA. *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 861 (Ill. 2005). Plaintiffs have alleged and factually supported with specificity all of these elements in their Complaint.

1. <u>Michaels' Conduct Was Deceptive</u>

Plaintiffs allege that Michaels is a retailer that accepts payment through credit and debit cards, that Michaels uses PIN pad terminals to process credit card transactions, and that when a PIN pad is properly operating, it securely transmits a cardholder's information to a transaction

---

Defendant cites stand for the proposition that because a defendant may have committed statutory consumer fraud violations in other states, an Illinois resident plaintiff is deprived of their ability to bring an ICFA cause of action. *See MacNeil Auto. Prods. Ltd v. Cannon Auto. Ltd*, No. 08-C139, 2009 WL 65498, at *6 n.4, 2009 U.S. Dist. LEXIS 1268 (N.D. Ill. Jan. 8, 2009) (where place of performance and delivery on contract was in the United Kingdom, expressing skepticism on application of ICFA based on choice-of-law analysis); *Landau v. CAN Financial Corp.*, 886 N.E.2d 405, 408 (Ill. App. Ct. 1st Dist. 2008) (dismissing ICFA claim brought by Pennsylvania resident premised on Defendant's corporate headquartering in Illinois). The argument is logically unsupported as well, as it would encourage those who wish to deceive consumers to do so on the widest scale possible to foreclose state by state consumer fraud act litigation. Furthermore, the circumstances that relate to the disputed transaction for the ICFA claims of the Illinois subclass *did* occur "primarily and substantially in Illinois" because Michaels failed to provide adequate security for PIN Pads in its Illinois stores, PIN Pad tampering occurred in Illinois, and each of the named Plaintiffs and all of the Illinois subclass members reside in Illinois and shopped at Michaels' retail locations in Illinois. *See* CAC ¶¶ 16 -19, 45.

manager or bank for verification to complete an in-store transaction such that the PIN pad protects cardholders from security breaches. CAC ¶¶ 21-22, 26, 44. Plaintiffs further allege that Michaels allowed widespread and systematic theft of customer financial information because it failed to employ appropriate technical, administrative and physical procedures (CAC ¶ 53) and that such failures deceived Michaels' customers – including Plaintiffs and the other Illinois Subclass members – because Michaels intended for those customers to rely on it to protect their credit and debit card information from unauthorized access. CAC ¶¶ 90-91. Nevertheless, Michaels failed to properly implement adequate, commercially reasonable security measures, and instead handled customer personal and financial information in such a manner that it was compromised. CAC ¶¶ 92-93. Plaintiffs further allege that Michaels' security failures benefited Michaels by providing savings on the costs of taking measures that would have prevented data from being compromised. CAC ¶¶ 52, 95.

In nearly analogous circumstances, these allegations have been held sufficient to state a claim for violation of the ICFA capable of withstanding a motion to dismiss. *See Richardson v. DSW, Inc.*, 05 C 4599, 2006 U.S. Dist. LEXIS 1840 (N.D. Ill. Jan. 18, 2006) ("*Richardson II*") (granting leave to amend ICFA cause of action dismissed in *Richardson I*). In *Richardson*, a data breach occurred at shoe retailer DSW, in which hackers stole customers' credit card information from DSW's computer systems. *See Richardson I*, at *1-2. In granting Plaintiffs leave to amend their complaint to assert an ICFA claim against DSW, Judge Manning ultimately rejected DSW's contention that it purportedly did not "benefit" from the allegedly wrongful conduct, *Richardson I*, at *15, holding that "DSW intentionally failed to follow security procedures mandated by its contracts with numerous credit card companies in order to save money and thus made its customer information vulnerable to hacking," and that "the benefit

accruing from DSW's allegedly intentional corner-cutting to conserve costs is enough to satisfy the benefit prong" of the IFCA. *Richardson II*, at *4. If anything, the facts here are even more compelling than in *Richardson*, because Plaintiffs in this case have actually had funds withdrawn from their bank accounts as a direct result of the security breach and Michaels' inadequate security practices.[11] Plaintiffs have alleged sufficient facts to support their claim that Michaels' operation as a retailer accepting credit cards with inadequate data security was the type of deception sufficient to support a "deceptive practices" claim under the IFCA.

2. Plaintiffs' ICFA Claim is Not Foreclosed by Their Breach of Implied Contract Claim

Michaels contends that Plaintiffs' cannot allege both a violation of the ICFA and breach of *implied* contract. Def. Mem. at 14-15. Yet, each of the cases Michaels cites in support of this argument involve *express* contracts that *both* parties agree govern their relationship.[12] Because Michaels disclaimed its obligation to implement reasonable and adequate data security measures

[11] None of the cases Michaels' cites in its attempt to recharacterize a merchant's gross failure to maintain reasonable and adequate security measures as non-deceptive support its contention. *See* Def. Mem. at 13-14. In *Johnson Prods. Co., Inc. v. Guardsmark, Inc.*, the court dismissed an ICFA claim brought by a hair care product manufacturer against the security company it hired guard its Chicago warehouse based on the security company's failure to guard because the security company's conduct was not a "broad misrepresentation to the public" that "reached the public generally." No. 97 C 6406, 1998 WL 102687, 1998 U.S. Dist LEXIS 2491, at *22 (N.D. Ill. Feb. 27, 1998). In *Kremers v. Coca-Cola Co.*, the Court dismissed Plaintiff's IFCA claim premised on Coca-Cola labeling its soft drink "Original Formula" even though it was sweetened with high fructose corn syrup instead of sucrose (as was used in Coca-Cola's 1886 original formula) because the named Plaintiff had never seen, and hence could never have been misled by, Coca-Cola's overt "Original Formula" label. 712 F. Supp. 2d 759, 769 (S.D. Ill. 2010). Finally, in *High Road Holdings, LLC v. Ritchie Bros. Auctioneers (Am.), Inc.*, the Court dismissed Plaintiff's IFCA claim because plaintiffs were not consumers and were not able to show any "consumer nexus" in an action primarily about an auctioneer's bid rigging. No. 1:07-cv-4590, 2008 WL 450470, 2008 U.S. Dist. LEXIS 11479, at *11 (N.D. Ill. Feb 15, 2008).

[12] *See* Def. Mem. at 14-15, citing *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 843-44 (Ill. 2005) (express written automobile insurance contract); *Greenberger v. GEICO Gen. Ins. Co.*, 631 F.3d 392, 399 (7th Cir. 2011) (same); *Zankle v. Queen Anne Landscaping*, 724 N.E.2d 988, 993 (Ill. App. Ct. 2d Dist. 2000) (express contract to perform landscaping services); *Sklodowski v. Countrywide Home Loans, Inc.*, 832 N.E.2d 189, 197 (Ill. App. Ct. 1st Dist. 2005) (express written mortgage note); *Western Howard Corp. v. Indian Harbor Ins. Co.*, No. 10-7857, 2011 WL 2582353, 2011 U.S. Dist. LEXIS 70069, at *13 (N.D. Ill. June 29, 2011) (express property insurance contract); *Duffy v. TicketReserve, Inc.*, 722 F. Supp. 2d 977, 980 (N.D. Ill. 2010) (express website user agreement).

to protect their customers' sensitive financial and personal data, dismissal of Plaintiffs' ICFA claim because Plaintiffs also assert a breach of implied contract claim is unwarranted.[13]

In addition, this case involves "more than the mere fact" that Michaels failed to fulfill its express contractual data security promises to Visa or implied contractual data security promises to consumers. *See Zankle*, 724 N.E.2d at 993. Plaintiffs' injuries are based on the additional fact of the data breach that flowed from Michaels' contractual violations. *See Richardson II*, 2006 U.S. Dist. LEXIS 1840, at *8 (allowing amendment to assert breach of ICFA claim after previously denying motion to dismiss breach of implied contract claim in *Richardson I*, explicitly rejecting applicability of the *Zankle* rule as plaintiff's "injury is based on illegal activity (the hacking) flowing from a breach of contract" and Plaintiff "is not basing her CFA claim solely on DSW's alleged breach of the contracts between DSW and the credit card companies"). Accordingly, Plaintiffs assertion of claims for violations of the ICFA and breach of implied contract co-exist harmoniously. Plaintiffs seek only a single recovery for their injuries and are permitted to pursue that recovery under through multiple causes of action.

3. Michaels' Conduct Was Also Unfair

In addition to providing consumers a remedy for deceptive practices, the ICFA also provides relief for unfair practices. In determining unfairness, "consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section

[13] Michaels' reliance on *Duffy*, 722 F. Supp. 2d 977, 991, to support its contention that Plaintiffs made a "mistake" in incorporating each of their foregoing allegations of their complaint into their ICFA and a breach of implied contract claims is equally misplaced. In *Duffy*, both parties claimed the existence of a contract that governed their relationship; here, where Michaels asserts that "no contract exists," Def. Mem. at 15, it cannot reasonably contend that Plaintiffs' ICFA claim is barred by their implied contract claim. Further, Michaels' obligations to maintain reasonable and adequate data security exist independently of its duties under the implied contract between customers and merchants in credit card transactions. *Cf. Duffy*, 722 F. Supp. 2d at 992 ("If [Defendant] has any duty to protect Plaintiffs . . . its obligations exist incident to its performance under the User Agreement."); *see also Shaw v. Hyatt Int'l Corp.*, 461 F. 3d 899, 902 (7th Cir. 2006) (dismissing plaintiffs ICFA claim where his "consumer fraud argument [] *relies exclusively on the express promises* made by" defendant) (emphasis added).

5(a) of the Federal Trade Commission Act." 815 Ill. Comp. Stat. 505/2.[14] In accord with the standards used by the FTC, to show that something is an "unfair practice" under the ICFA, the practice must (1) offend public policy; (2) be immoral, unethical, oppressive, or unscrupulous; or (3) cause substantial injury to consumers. *Robinson*, 775 N.E.2d at 961 (adopting test from *Cheshire Mortgage Service, Inc. v. Montes*, 612 A.2d 1130, 1143 (Conn. 1992)); *see also Siegel v. Shell Oil Co.*, 612 F.3d 932, 935 (7th Cir. 2010) (noting a substantial injury is one that must "(1) be substantial; (2) not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and (3) be an injury that consumers themselves could not reasonably have avoided."). "'All three criteria do not need to be satisfied to support a finding of unfairness. A practice may be unfair because of the degree to which it meets one of the criteria or because to a lesser extent it meets all three.'" *Robinson*, 775 N.E.2d at 961.

Plaintiffs' allegations concerning Michaels' cost-cutting on data security and the results thereof satisfy the unfairness criteria. The data breach here involved the compromise of thousands of individuals' information, causing them substantial and widespread damage. In a similar data breach case, the First Circuit noted:

> a court using these general FTC criteria might well find in the present case inexcusable and protracted reckless conduct, aggravated by failure to give prompt notice when lapses were discovered internally, and causing very widespread and serious harm to other companies and to innumerable consumers. And such conduct, a court might conclude, is conduct unfair, oppressive and highly injurious.

[14] Michaels puzzlingly suggests that because there is no private right of action under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a), acts that would violate the FTCA cannot form the basis of an ICFA cause of action, *see* Def. Mem. at 16. That suggestion is contradicted by the plain language of Section 2 of the ICFA.

See Amerifirst Bank v. TJX Cos. (In re TJX Cos. Retail Sec. Breach Litig.), 564 F.3d 489, 496 (1st Cir. 2009). Thus, under the FTC's standards, Michaels' insufficient data security, as alleged in the Complaint, constitutes an unfair practice under the ICFA.

Further, the FTC has consistently and repeatedly brought enforcement actions against companies "with security deficiencies in protecting sensitive consumer information," alleging that they have failed to use "reasonable and appropriate security measures" to prevent unauthorized access to personal information stored on computer networks for violations of the FTCA. *See In re Hannaford Bros.*, 613 F. Supp. 2d at 130 (noting FTC "complaints 'charging companies with security deficiencies in protecting sensitive consumer information.'") (footnote omitted); *see also In re TJX*, 564 F.3d at 496 ("[W]e do not think irrelevant the host of FTC complaints and consent decrees condemning as 'unfair conduct' specific behavior similar to that charged by plaintiffs," which was "the theft from TJX computers of customer credit and debit card information and the subsequent fraudulent use of the information"). Indeed, all of the complaints underlying the FTC Decisions and Orders cited by Michaels charge that the various companies' failures to provide reasonable and appropriate data security constitute deceptive or unfair trade practices under the FTCA.[15] Plaintiffs' allegation that Michaels failed to provide reasonable and appropriate data security, and the fact that this conduct constitutes an unfair trade practice, *see* CAC ¶ 51-52, is a well-pleaded fact the Court must accept as true.

Moreover, Michaels' argument that Plaintiffs have not alleged that "Michaels was ever *determined to be* PCI DSS non-compliant before or during" the data breach, Def. Mem. at 17

[15] "Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace." Prepared Statement of the Federal Trade Commission on Data Security Before the Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, U.S. House of Rep. (Jun. 15, 2011) (Prepared Statement of FTC Comm'r Edith Ramirez), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf.

(emphasis added), misses the point – as Plaintiffs clearly and directly allege that Michaels *was* non-compliant with PCI PIN requirements. CAC ¶¶ 4, 51-52. Michaels' non-compliance is supported by Plaintiffs' specific factual allegation (and Michaels' own admissions[16]) that PIN Pads in Michaels stores were breached over a period of nearly four months. *See* CAC ¶¶ 45-47. Had Michaels maintained reasonable and appropriate data security practices, Michaels could have better protected its customers from security breaches like the one at issue here. *See* CAC ¶ 44. Michaels' argument that Plaintiffs must cite even more facts as to *how* Michaels' PIN pads were non-compliant vastly overstates Plaintiffs' pleading burden.

D. Plaintiffs Adequately Alleged that Michaels' Notice was Statutorily Deficient under the Illinois Personal Information Privacy Act

Plaintiffs adequately allege that both the timing and manner of Michaels' notice was deficient under the Illinois Personal Information Protection Act ("PIPA"). PIPA requires that a data collector such as Michaels provide notice to Illinois residents following a data breach "in the most expedient time possible and without reasonable delay, consistent with any measures necessary to determine the scope of the breach" and that failure to do so constitutes an unfair trade practice under the ICFA. *See* 815 Ill. Comp. Stat. 530/10; 815 Ill. Comp. Stat 530/20. While Michaels urges the Court to believe that it remained oblivious throughout the course of the breach and that it provided expedient and timely notice as soon as it knew of the breach, the matter of when Michaels actually knew of the data breach is a contested issue of fact for

[16] Michaels' contention that Plaintiffs have not and cannot allege that the PIN Pads in Michaels stores were PCI-noncompliant is contradicted by the Complaint, *see* CAC ¶ 51, and by Michaels' own admission that "tampered payment card terminals were placed by unauthorized individuals in certain Michaels stores." Michaels' Notice to Our Customers (May 25, 2011) available *at* http://demandware.edgesuite.net/aaeo_prd/on/demandware.static/Sites-Michaels-Site/Sites-Michaels-Library/default/v1313729955335/documents/press-releases/052911-Notice-to-Our-Customers.pdf. A tampered PIN pad is clearly non-compliant. *See* CAC ¶ 32 (citing PIC PIN Security Requirement 1: "All cardholder-entered PINs are processed in equipment that conforms to the requirements for tamper-resistant security modules.").

discovery. The fact that Plaintiffs cite Michaels' own self-serving statements regarding when Michaels claims to have become aware of the data breach is not a concession as to when Michaels actually became aware of the breach. *See* CAC ¶¶ 8-9, 45, 47, 56-61; *cf.* Def. Mem. at 2, 20. On a motion to dismiss, Michaels has no grounds to challenge Plaintiffs' factual allegations that Michaels did not provide "timely or effective notice." CAC ¶¶ 16-19, 99.

Additionally, Plaintiffs alleged that Michaels provided notice only to a small subset of affected Illinois residents following public reports of the breach to Illinois law enforcement authorities. *See* CAC ¶¶ 8, 54-61. By failing to conspicuously notify all affected Illinois residents affected by the data breach, Michaels' notice fell short of the requirements of PIPA. *Id* at. ¶¶ 98-100. Michaels attempts to avoid its obligation to directly provide written notice to Plaintiffs and the class by claiming that it was entitled to provide substitute notice pursuant to 815 Ill. Comp. Stat. 530/10(c)(3).[17] But Michaels cannot show that it has a right to provide substitute notice based on the allegations of the complaint, as Michaels has not met its statutory burden of demonstrating "that the cost of providing [written or electronic] notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information." *See* 815 Ill. Comp. Stat. 530/10(c)(3). Nor has Michaels established that it "maintains its own notification procedures as part of an information security policy[.]" *See* 815 Ill. Comp. Stat. 530/10(d). Thus, Michaels' argument that it is entitled to rely solely on its provision of substitute notice – which Plaintiffs contend was

[17] Michaels' reliance on *Cooney* in support of its "PIPA compliance" argument is thus misplaced. In *Cooney*, the defendant "sent a letter" to each of the individual employees whose personal information was compromised in the data breach and did not (and could not) rely on substitute notice to fulfill its PIPA notice obligations. *See Cooney*, 943 N.E. 2d at 27-28. None of the Plaintiffs in this case received a notification of the breach from Michaels. *See* CAC ¶¶ 16-19.

woefully and misleadingly uninformative regardless, *see* CAC ¶¶ 57-60 – does not show that Michaels fulfilled its duties under PIPA.

Plaintiffs further allege that the content of Michaels' notice was insufficient as well. *See* CAC ¶ 57 (Michaels "intentionally and misleadingly underplayed the severity of the data breach situation."). While PIPA only minimally prescribes the contents of a data breach notice, at the very least, a data collector must disclose "*that there has been* a breach of the security of the system data[.]" *See* 815 Ill. Comp. Stat. 530/10(a). Here, Michaels repeatedly stated that there "may have been" a data breach. CAC ¶ 57. Failure to affirmatively acknowledge the very existence of the breach calls into question the effectiveness of the required notice[18] and demonstrates Michaels' failure to comply with PIPA. Accordingly, Plaintiffs have properly alleged Michaels' violation of the PIPA, and hence Michaels' additional commission of an unfair trade practice under the ICFA.

E. Plaintiffs Sufficiently Plead Their Negligence Claim

To state a claim for negligence under Illinois law, a plaintiff must allege "the existence of a duty of care owed by the defendant to the plaintiff, a breach of that duty, and an injury proximately caused by that breach." *Ward v. K Mart Corp.*, 554 N.E.2d 223, 143 (Ill. 1990). Whether defendant owed plaintiff a duty of reasonable conduct is a question of law for the court to determine. *Estate of Johnson v. Condell Mem'l Hosp.*, 520 N.E.2d 37 (Ill. 1988). In determining whether a duty exists, reasonable foreseeability of harm is the primary concern but the court must also consider the likelihood of injury, the magnitude of the burden to guard

[18] Regardless of whether facial notice is provided, courts should examine whether such notice is effective in providing information to consumers. *See Kaufman v. Am. Express Travel Related Servs. Co.*, No. 07-C1707, 2008 U.S. Dist. LEXIS 18129, at *18-19 (N.D. Ill. Mar. 7, 2008) (rejecting motion to compel arbitration in gift card case and noting "In light of the inconsistency of terms and relative obfuscation of documentation, the court questions whether *effective* notice was provided to Kaufman, notwithstanding American Express's *facial* compliance with notice requirements.") (emphasis in original).

against the injury, and the consequence of placing the burden on defendant. *Kirk v. Michael Reese Hosp. & Med. Ctr.*, 513 N.E.2d 387 (Ill. 1987).

Here, Plaintiffs have sufficiently alleged that Michaels had a duty to act responsibly – including following industry standards – to protect class members' sensitive personal and financial information, CAC ¶¶ 7, 26, 33, 37, 44; that Michaels' inadequate security measures constitute a breach of that duty, CAC ¶¶ 51-53; that Michaels' inadequate security was a proximate cause of the security breach; and that as a result of Michaels' negligence, Plaintiffs were damaged, CAC ¶¶ 51-53, 104-11. Given the spate of data breaches in recent years, the harm from inadequate data security is plainly foreseeable. Furthermore, because Michaels, and not consumers, controls the implementation of data security measures, the burden of preventing injuries caused by inadequate data security properly falls on Michaels.

The cases Michaels cites in an attempt to disclaim its duty to reasonably protect sensitive consumer credit and debit card information are distinguishable. In *Cooney*, the court did not find that defendant had a duty to protect sensitive personal information based solely on PIPA and HIPAA. *See Cooney*, 943 N.E. 2d at 27-28 ("Because the provisions in the [PIPA] are clear, we must assume it reflects legislative intent to limit defendants' duty to providing notice."). In this case, however, Michaels' duty derives from its responsibility to consumers and issuing banks to reasonably handle credit and debit card transactions.

Plaintiffs sufficiently allege that Michaels' failure to implement appropriate data security measures made "its customers easy targets for theft and misuse of their financial information, including in the manner undertaken by the Skimmers here" and that such consequences were foreseeable. CAC ¶ 53, 94. When criminal conduct is reasonably foreseeable, "the causal chain is not necessarily broken" by criminal intervention between a defendant's ICFA violation and a

plaintiff's injury. *Petrauskas v. Wexenthaller Realty Mgm't, Inc.*, 542 N.E.2d 902, 909 (1st Dist. 1989) (internal citations omitted). Thus, Plaintiffs' allegations are sufficient to show Michaels' ongoing failures to provide reasonable and adequate data security proximately caused Plaintiffs' injuries. *See also Richardson II*, 2006 U.S. Dist. LEXIS 1840, at *7 ("Given the procedural posture of this case, the court cannot find that the hacking incident was unforeseeable as a matter of law, so Richardson's new allegations support a cause of action based on the CFA.").[19] Having already established injury, Plaintiffs have satisfied their pleading burden for all of the elements of a negligence claim.

F. The Economic Loss Rule Does Not Bar Plaintiffs Negligence Claim

Michaels' contention that Plaintiffs' negligence claim is barred by Illinois' "economic loss rule," Def. Mem. at 21, is incorrect. As discussed below, several exceptions to the economic loss doctrine apply here. Contrary to Michaels' suggestion, the economic loss rule is not a broad rule that bars recovery for purely economic losses in tort cases. Rather, the economic loss doctrine generally bars tort claims for pecuniary damage resulting from breach of a contract.[20] The doctrine's rationale is that "parties to a purely commercial transaction should not be able to recover in tort for economic losses arising out of that transaction when the parties have

[19] The proximate cause cases that Michaels' cites are readily distinguishable. In *Guin v. Brazos Higher Educ. Serv. Corp., Inc.*, the court specifically found that the burglary of a laptop containing sensitive information from defendant's employee's home was not reasonably foreseeable precisely because the employee "took necessary precautions to secure his house from intruders." No. 05-668, 2006 U.S. Dist LEXIS 4846, at *12 (D. Minn. Feb. 7, 2006). And in *Altepeter v. Virgil State Bank*, a case involving a claim by a bank customer injured during a robbery against the bank for failing to maintain adequate security, the Court found that the customer failed to state a cause of action because "no facts are alleged from which any one could conclude that defendant did not discharge this duty to plaintiff." 104 N.E.2d 334, 337 (App. Ct. Ill. 2d Dist. 1952). Here, Plaintiffs have specifically alleged how Michaels failed to take necessary precautions to protect Plaintiffs' data in that Michaels was non-compliant with industry standards. CAC ¶ 51, 109.

[20] *See Rich Prods. Corp. v. Kemutec Inc.*, 241 F.3d 915, 917-18 (7th Cir. 2001); *Moorman Mfg. Co. v. National Tank Co.*, 435 N.E.2d 443, 449 (Ill. 1982).

negotiated and the UCC provides for adequate contract remedies." *Twin Disc. Inc. v. Big Bud Tractors, Inc.*, 772 F.2d 1329, 1332 (7th Cir. 1985).

Courts have held the economic loss doctrine does ***not*** apply where the defendant is alleged to have breached a duty owed independent of any contractual obligation or warranty.[21] Such is the case here. Indeed, Plaintiffs have alleged Michaels owed Plaintiffs an independent duty to implement reasonable and adequate security measures in addition to any express contractual obligation duties owed to Plaintiffs and that Michaels breached those duties. *See* CAC ¶¶ 106-08. Here, Plaintiffs and the other Class members were unprotected parties, not in express contractual privity with Michaels and without the ability to negotiate the adequacy of Michaels' data security practices, that sustained damages resulting from Michaels' mishandling of their sensitive personal and financial information.[22] Indeed, under analogous circumstances, the economic loss doctrine has been deemed inapplicable. *See, e.g., Choi v. Chase Manhattan Mortg. Co.*, 63 F. Supp. 2d 874, 884 (N.D. Ill. 1999) ("'Tort law . . . applies in situations where

[21] *See Hinkle Eng'g, Inc. v. 175 Jackson LLC*, No. 01-C5078, 2001 WL 1246757, at *3 (N.D. Ill. Oct. 18, 2001); *Serfecz v. Jewel Food Stores, Inc.*, No. 92-C4171, 1998 WL 142427, at *2-5 (N.D. Ill. Mar. 26, 1998) (duty not to commit waste arose independent of contract); *see also Mutual Serv. Cas. Ins. Co. v. Elizabeth State Bank*, 265 F.3d 601, 617-18 (7th Cir. 2001) (where breach of duty arises outside of contract in Illinois, economic loss rule does not bar recovery in tort); *Harrison v. Dean Witter Reynolds, Inc.*, 715 F. Supp. 1425, 1433 (N.D. Ill. 1989) ("the [Illinois Supreme] Court never actually has ruled that the [economic loss] doctrine extends to cases in which the defendant has extra-contractual duties"), *aff'd in part, rev'd in part on other grounds*, 974 F.2d 873 (7th Cir. 1992).

[22] By contrast, almost all of the cases Michaels cites involve parties to commercial or consumer transactions who had contractual or warranty remedies, *see* Def. Mem. at 21-22, and are thus inapposite. Only one case upon which Michaels relies – *Donovan v. Cnty. Of Lake*, No. 2-10-0390, 2011 Ill. App. LEXIS 733 (Ill. App. 2d Dist., July 8, 2011) – that applied the economic loss rule did not involve parties to such transactions and that case involved a dispute between residents of a housing subdivision against Lake County to stop that County from issuing revenue bonds to construct a new water system, asserting negligence claims based on facts completely dissimilar, and thus distinguishable, from those asserted here.

society recognizes a duty to exist wholly apart from any contractual undertaking'") (citation omitted).[23]

Finally, Michaels also fails to confront Plaintiffs' allegations of Michaels' "willful[]" conduct, CAC ¶¶ 93-94, and its "reckless indifference toward the rights of others," CAC ¶ 102, which also render the economic loss rule inapplicable here.[24]

G. Plaintiffs Sufficiently Plead Their Negligence *Per Se* Claim

Michaels' arguments against Plaintiffs' negligence *per se* claim are premised entirely on their arguments disclaiming violations of the SCA, ICFA, FTCA, and PIPA. Given that Plaintiffs have alleged sufficient facts to show Michaels' violation of these statutes, all of which were designed to protect consumers like Plaintiffs from the type of harm that occurred here, Defendant's arguments are without merit.[25] Furthermore, the fact that Plaintiffs seek only a single recovery under multiple theories does not discount the propriety of their pleading multiple causes of action arising from the same wrongful conduct. *See Majcher v. Laurel Motors, Inc.*, 680 N.E.2d 416, 429 (Ill. App. Ct. 2d Dist. 1997) (where plaintiff had received judgment for

---

[23] *See also Hinkle Eng'g, Inc.*, 2001 WL 1246757, at *3; *Serfecz*, 1998 WL 142427, at *2-5.

[24] *See Dundee Cement*, 712 F.2d 1166, 1170 (7th Cir. 1983) (economic loss rule inapplicable where plaintiff alleges intentional harm); *Kleebatt v. Bus. News Publ'g Co.*, 678 F. Supp. 698, 702-03 (N.D. Ill. 1987) (economic loss risk inapplicable to willful and wanton misconduct claim where "plaintiffs' 'commercial expectations' were irrelevant" and where the defendants acted recklessly and intentionally).

[25] Michaels' inconsistently argues that because the FTCA *does not* provide a private right of action, its violation cannot form the basis of a negligence *per se* claim, and that because the SCA and ICFA *do* provide a private cause of action, they also cannot provide the basis for a negligence *per se* claim. But the existence of a private right of action is irrelevant to the question of whether a statute imposes a duty of care and whether a violation of the statute demonstrates a rebuttable presumption of breach of that duty when a cause of action (such as negligence) exists at common law, as that is the entire purpose of the negligence *per se* doctrine. *See Cuyler v. United States*, 362 F.3d 949, 952 (7th Cir. Ill. 2004) ("The doctrine of negligence *per se* . . . provides that where a cause of action does exist at common law, the standard of conduct to which a defendant will be held may be defined as that required by statute, rather than as the usual reasonable person standard. . . . [A]n accurate statement of Illinois law is that in Illinois the violation of a statutory standard of care is prima facie evidence of negligence rather than negligence *per se*.") (citations and quotations omitted).

both statutory odometer fraud and common law fraud arising from same injury, satisfaction of the greater judgment satisfied both).

H. Plaintiffs Sufficiently Plead Their Breach Of Implied Contract Claim

A claim for breach of contract implied in fact requires proof of the same elements as breach of an express contract – that is an offer, acceptance, and consideration – as well as a meeting of the minds. *See Brody v. Finch Univ. of Health Sci./The Chicago Med. Sch.*, 698 N.E.2d 257, 265 (Ill. App. Ct. 2d Dist. 1998) *citing Foiles v. North Greene Unit Dist. No. 3*, 633 N.E.2d 24, 27 (Ill. App. Ct. 4th Dist. 1994).

In this case Plaintiffs sufficiently plead their breach of implied contract claim. Michaels offered to accept credit and debit cards swiped through PIN Pads in Michaels Stores from customers as a form of payment; Plaintiffs accepted Michaels' offer by swiping their cards through Michaels' PIN pads, consideration of payment and merchandise was exchanged between the parties; and, as Plaintiffs allege, Michaels and Plaintiffs mutually agreed that Michaels would handle Plaintiffs credit and debit card information reasonably. *See, e.g.*, CAC ¶¶ 2, 16-19, 21-22, 26-38, 62-63, 118- 125.

In any credit or debit card transaction, there are contractual obligations implied between the parties. Denying a motion to dismiss a breach of implied contract claim in circumstances analogous to this case, Judge Manning explained the consumer-retailer implied contract:

> The court begins with the premise that DSW's acceptance of non-cash payments led to the creation of a contractual relationship between DSW and its customers. As then Chief Justice Burger noted in a dissent that was premised on a legal argument unconnected to his summary of how credit cards work, 'bank credit card systems . . . rely upon a three-way transaction between the card issuer, the cardholder, and a subscribing retailer. This tripartite credit card arrangement basically entails three separate contractual agreements: (1) between the bank issuing the credit card and the individual cardholder; (2) between one of the banks in the system and a local merchant; and (3) between the merchant and the cardholder.' *U. S. v. Maze*, 414 U.S. 395, 413 n.2, 94 S. Ct. 645, 38 L. Ed. 2d 603 (1974) (Burger, CJ, dissenting). ***The court thus disagrees with DSW's claim that***

> ***its acceptance of non-cash methods of payment does not lead to the creation of some sort of contractual relationship between DSW and its customers. The contours of this relationship are unclear at this point in the proceedings, but the basic fact remains that DSW and its non-cash paying customers have a contractual relationship.***

Richardson I, at *5-6 (emphasis added). Further, given that it is likely that Michaels accepts some form of payments (such as credit cards, as alleged in the complaint) and not others, it would be possible for a jury to find that as part of Michaels' offer to accept credit cards for payment, Michaels also offered "to take reasonable measures" to keep Plaintiffs' credit card information secure. *See id.*, at *10.

Michaels' arguments regarding the "implausibility" of an implied contract in credit and debit card processing, based on an apparent lack of mutual intent to contract, Def. Mem. at 24, is thus belied by both case law and common sense. Clearly, when a customer tenders a credit card to a merchant, it is an implied element of that transaction that "the merchant will not use the card for other people's purchases, will not sell or give the data to others (except in completing the payment process), *and will take reasonable measures to protect the information (which might include meeting industry standards*), on the basis that these are implied commitments[.]" *Hannaford*, 613 F. Supp. 2d at 119 (emphasis in original, footnote omitted).

In any event, whether the merchant and consumer had a meeting of the minds as to the terms of their implied contract "is not an appropriate argument to raise at the motion to dismiss stage as the court cannot make any findings of fact as to what the parties did or did not believe." *Richardson I*, 2005 U.S. Dist. LEXIS 26750, at *6-7. Accordingly, Plaintiffs have sufficiently stated a claim for breach of implied contract, and Michaels' motion to dismiss this count of the Complaint should thus be denied.

I. Plaintiffs Adequately Allege Michaels' Violations of the Stored Communications Act

The Stored Communications Act, 18 U.S.C. § 2702 ("SCA") governs the unauthorized disclosure of electronic communications maintained on computers. Congress recognized that the information in electronic communications "may be open to possible wrongful use and public disclosure. . ." and enacted the SCA in part "to protect individuals' privacy interests in personal and proprietary information." *Id*. Plaintiffs' allegations satisfy each of the relevant requirements of the SCA.

1. The SCA Applies to Michaels

In their Complaint, Plaintiffs allege that Michaels violated 18 U.S.C. § 2702(a)(1), which provides that "a person or entity providing an electronic communications service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." CAC ¶¶ 76-78, 84, 86. In addition, or in the alternative, Plaintiffs also allege that Michaels violated 18 U.S.C. § 2702(a)(2), which provides that "a person or entity providing remote computing services to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service." CAC ¶¶ 81-84, 86. Plaintiffs adequately allege that both provisions apply to Michaels.

2. Michaels Provides Electronic Communications Services

As set forth in 18 U.S.C. § 2702(a)(1), an "electronic communications service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). An "electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnet, photoelectronic or photooptical system that affects interstate or foreign commerce . . .." 18 U.S.C. § 2510(12).

Michaels provides an "electronic communications service to the public," as provided in 18 U.S.C. § 2702(a)(1), because it provides consumers at large with credit and debit card payment processing capability that enables customers who purchase merchandise at Michaels to send or receive wire or electronic communications concerning their account data and PINs to transaction managers, card companies or banks. CAC ¶ 78. Debit and credit card purchases at Michaels are effectuated through transmission of the customer's card information from the Michaels PIN pad to a transaction manager or bank for verification to complete the sale, and the receipt of authorization for the sale. *Id*. at ¶¶ 22, 25; *see also Devine v. Kapasi*, 729 F. Supp. 2d 1024, 1026-1027 (N.D. Ill. 2010) (a network that provides authorized users with the ability to send and receive electronic communications through password-protected accounts is an electronic communications service); *Kaufman v. Principal Connections, Ltd.*, No. 05-CV6782, 2006 U.S. Dist. LEXIS 71104, at *19-20 (S.D.N.Y. Sept. 27, 2006) (an online business which provides its customers with the means to engage in private communications with third parties may constitute an electronic communications service).[26] These allegations are sufficient at the dismissal motion stage and Michaels' claim that it does not provide electronic communication services is, at best, premature. *See Lopez v. First Union Nat'l Bank*, 129 F.3d 1186, 1189-1190 (11th Cir. 1997). ("[Defendant contends] it is not an electronic communication service. We reject that contention which amounts to nothing more than a denial of the allegations in Lopez's complaint"); *Becker v. Toca*, No. 07-7202, 2008 U.S. Dist. LEXIS 89123, at *2, 12-13 (E.D. La. Sept. 26, 2008) ("It would be premature or speculative for the Court to dismiss" plaintiff's SCA

[26] Michaels relies on two district court cases concerning airlines, each of which held that airlines are not ECS providers based on their computerized reservation (and payment) systems. *See Dyer v. Nw. Airlines Corp*., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004); *In re Jetblue Airways Corp. Privacy Litig*., 379 F. Supp. 2d 299, 307, 310 (E.D.N.Y. 2005). But the Ninth Circuit has ruled that an airline provides an electronic communications service through its computerized reservation system. *See U.S. v. Mullins*, 992 F.2d 1472, 1474, 1478 (9th Cir. 1993). The trial court opinions are less persuasive than the Ninth Circuit's opinion in *Mullins*, and both disregard the unambiguous language of 18 U.S.C. § 2510(15).

claim under 18 USC § 2701 where the same definition of "electronic communication service" was at issue). *See also H & R Block E. Enters. v. J & M Sec.*, LLC, No. 05-1056-CV, 2006 U.S. Dist. LEXIS 26690, at *9-10 (W.D. Mo. Apr. 24, 2006) ("Plaintiff's allegation that "H&R Block provides electronic communication services … is sufficient to state a claim. After discovery, the Court will be inclined to apply the cited cases to the undisputed facts.").

Much of Michaels' support for its contention that merchants do not provide electronic communications services is derived from cases adopting a disfavored and overly narrow definition of the term. For example, Michaels cites *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001). However, that opinion relies on *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998), upon which Michaels also relies. *Andersen* held that an internal corporate email system was not an electronic communications service, but that decision is at odds with the weight of more recent cases holding that email services are covered by the SCA.[27] Michaels' citation to *Ipreo Holdings, LLC v. Thomson Reuters Corp.*, No. 09 CV 8099 (BSJ), 2011 WL 855872, at *6 (S.D.N.Y. Mar. 8, 2011) is likewise inapposite because the plaintiff in that case alleged that the electronic communications service at issue was an electronic bulletin board. Plaintiff makes no such allegation here.

3. Michaels Provides Remote Computing Services

As applied in 18 U.S.C. § 2702(a)(2), the term "remote computing service" means "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). An "electronic communications system" is

[27] It is also well-established that e-mail services are electronic communications services. *See, e.g., U.S. v. Warshak*, 631 F.3d 266, 282 (6th Cir. 2010); *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2003). As the court in *Cornerstone Consultants, Inc. v. Production Input Solutions, LLC*, No. C 10-3072, 2011 U.S. Dist. LEXIS 55009, at *57-59, *68-70 (N.D. Iowa May 19, 2011), reasoned, such a conclusion "is more consistent with the definition of 'electronic communication service' in 18 U.S.C. § 2510(15)."

defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14). Plaintiffs allege that Michaels provides remote computing services to the public through its payment processing equipment, including its PIN pad terminals, because such equipment is used for the electronic storage and remote processing of customer payment card information during the payment verification process. CAC ¶¶ 81-84. Plaintiffs' allegations are consistent with the language of the statute and are demonstrably true.

4. Michaels Knowingly Divulged Plaintiffs' Personal Information

Plaintiffs set forth detailed allegations that Michaels' conduct was knowing because the risks of a data breach were well-known, and were preventable had Michaels complied with its known contractual obligations and industry security standards. To "knowingly divulge" information in violation of the SCA requires only that the defendant was (i) aware of the nature of the conduct, (ii) aware of or possessing a firm belief in the existence of the requisite circumstances; and (iii) an awareness of or a firm belief about the substantial certainty of the result. *See Freedman v. Am. Online, Inc.*, 329 F. Supp. 2d 745, 748 (E.D. Va. 2004).

Plaintiffs allege, in detail, that Michaels' security measures failed to comply with its known contractual obligations and industry standards, that Michaels knew the risks of failing to do so, and that Michaels breached those obligations in order to cut costs. CAC ¶ 52. Plaintiffs also allege that Michaels was aware that its customers' personal and financial information would be divulged to third parties because its security systems failed to comply with contractual requirements and industry standards, and because its conscious failure to comply in the interest of cost cutting posed "an extremely high level of risk" that customer information would be

exposed. *Id.* ¶ 34. Accordingly, these allegations support an inference that Michaels knew that its customers' personal and financial information could and would be accessed by third parties.

Michaels cites *Muskovich v. Crowell*, No. 3-95-CV-20007, 1996 U.S. Dist. LEXIS 22634, at *13-14 (S.D. Iowa Aug. 30, 1996) for the proposition that a defendant's lax security cannot establish the requisite scienter to state an SCA claim, but that case says nothing of the sort. Indeed, *Muskovich* was decided on a motion for summary judgment based on documents outside the pleadings. *Id.* Only after the defendants presented evidence of the security measures actually employed, did the Court determine that the defendants' conduct did not create a substantial certainty that plaintiffs' information would be compromised. *See id*., at *14 (citing documents in support of motion).

Michaels' reliance on *Freedman* is similarly misplaced. The case was also decided on summary judgment and the court found that the defendant's conduct met the scienter requirement. While the court in *Bansal v. Server Beach*, 285 F. App'x 890 (3d Cir. Pa. 2008), was decided on a motion to dismiss, the defendant had a complete defense that no amount of discovery could have overcome: the plaintiffs' information was disclosed to a government agency pursuant to court order. *See id.* at 892. Such conduct is explicitly permitted under the SCA. *See id.; see also* 18 U.S.C. § 2707(e). In this case, however, Michaels has no such defense. Moreover, Michaels has not disclosed the method by which the Plaintiffs' and other Class members' personal financial information in at least eighty stores across the United States was compromised. This information can only be obtained through appropriate discovery.

5. Class Members' Personal Financial Information Is The Contents Of A Communication

The SCA prohibits the exposure of the contents of stored communications, providing that "contents" includes "any information concerning the substance, purport, or meaning of that

communication." 18 U.S.C. § 2510(8). Plaintiffs' magnetic strip information and PIN numbers constitute the contents of the transactions at issue.

Here, Plaintiffs allege that customers swiped their credit and debit cards through Michaels' PIN pad terminals and then entered their PINs associated with their accounts. CAC ¶¶ 21-22. The PIN pad terminal then encrypted the cardholder's PIN, temporarily stored the encrypted PIN and other card information from the card's magnetic stripe, and transmitted that information to a transaction manager or bank for verification to complete the transaction. *Id.* at ¶¶ 21-25. Plaintiffs further allege that Class members' credit and debit card information and PIN numbers were obtained and used, for among other reasons, to make unauthorized withdrawals from customers' bank accounts and unauthorized purchases of merchandise. *Id.* at ¶¶ 1-3, 6, 16-19, 21-25. In this case, the Class members' debit and credit card information, their PINs and other information from the magnetic stripe are the "contents" of the communication. Plaintiffs' interpretations is consistent with the Eleventh Circuit's decision in *Lopez*, which reversed dismissal of claims arising under 18 U.S.C. § 2702 where plaintiffs alleged that their banks disclosed the contents of electronic funds transfers. *See Lopez*, 129 F.3d at 1188.

Michaels' attempt to carve out credit and debit card numbers and PIN numbers from the definition of "contents" under the SCA is unpersuasive and unsupported. Moreover, Michaels' reliance on 18 U.S.C. § 2510(12)(D) is misplaced, as that section applies to "electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." However, the information at issue here was stored not by a financial institution, but by Michaels.

Finally, Defendant cites no case applying this statute to exclude personal financial information from the ambit of the SCA. For instance, in *In re Application of the United States of*

America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 306 (3d Cir. 2010), the government sought information regarding "the location of the antenna tower and, where applicable, which of the tower's 'faces' carried a given call at its beginning and end," as opposed to confidential financial information that could be used to commit identity theft. Similarly, *Hill v. MCI Worldcom Comm'cns, Inc*., 120 F. Supp. 2d 1194, 1195 (S.D. Iowa 2000), is likewise unpersuasive. That case distinguishes call details (such as number called, date, time, length of call, names, addresses and phone numbers of parties on the call) from the contents – the words spoken – of the call. *Hill*, 120 F. Supp. at 1195-96.[28] Unlike the Eleventh Circuit's decision in *Lopez*, the cases Michaels relies on here have nothing to do with electronic funds transfers. *See Lopez*, 129 F.3d at 1188. Michaels' proposed exception of consumers' debit and credit card information from the ambit of the SCA would swallow the rule, and render the SCA statute inapplicable to the personal and financial information Congress sought to protect in enacting the statute.

6. The SCA Provides for Statutory Damages Absent a Showing of Actual Damages

A review of the pertinent legislative history clearly demonstrates shows that actual damages are not necessary for an award of statutory damages under the SCA. *See* H.R. Rep. No. 99-647, p. 74 (1986) ("[d]amages [under 18 U.S.C. § 2707(c)] include actual damages, any lost profits but in no case less than $1,000"). In *Konop v. Hawaiian Airlines, Inc.*, 411 B.R. 678, 683 (D. Haw. 2009) *aff'd* 401 F. App'x 242 (9th Cir. 2010), the plaintiff, who did not present evidence of actual damages or violator profits, was still entitled to statutory damages. Similarly,

[28] Michaels' citation to the unpublished opinion of *Kathrein v. McGrath*, 166 F. App'x 858 (7th Cir. 2006) must be disregarded. *Kathrein* is also distinguishable because the plaintiff in that case did not dispute that he failed to adequately allege a claim arising under the SCA. *Id*., at 863.

in *Cedar Hill Assocs., Inc. v. Paget*, No. 04-C0557, 2005 U.S. Dist. LEXIS 32533, 2005 WL 3430562, at *3 (N.D. Ill. Dec. 9, 2005), the court cited the legislative history of the SCA in determining that the limitation on liquidated damages in the Privacy Act is inapplicable to the SCA). The same result was reached in *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 759 F. Supp. 2d 417, 427 (S.D.N.Y. 2010) ("Defendants are accordingly entitled to the statutory minimum of $1,000 per violation of the statute, whether or not they have suffered actual damages.").

Finally, as noted in *Pure Power*, Michaels' reliance on *Van Alstyne v. Elec. Scriptorium, Ltd*., 560 F.3d 199, 204-06 (4th Cir. 2009) is misplaced. *See Pure Power*, 759 F. Supp. 2d at 427. The *Pure Power* court recognized that the court in *Van Alstyne* misinterpreted the Supreme Court's decision in *Doe v. Chao*, 540 U.S. 614 (2004), which held that statutory damages under the Privacy Act, not the SCA, cannot be recovered absent actual damages. *Id.* at 427. Here, plaintiffs bring a claim under the SCA and have also sufficiently pled actual damages.

IV. CONCLUSION

For all of the foregoing reasons, Plaintiffs respectfully submit that this Court deny Defendant's Motion to Dismiss.

Dated: September 9, 2011

Respectfully submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC

By: /s/ Adam J. Levitt
Adam J. Levitt (ARDC#06216433)
Edmund S. Aronowitz (ARDC#6304587)
55 West Monroe Street, Suite 1111
Chicago, Illinois 60603
Tel: 312-984-0000
Fax: 312-984-0001
levitt@whafh.com
aronowitz@whafh.com

Scott A. Bursor (*pro hac vice*)
Joseph I. Marchese (*pro hac vice*)
BURSOR & FISHER, P.A.
369 Lexington Avenue, 10th Floor
New York, New York 10017
Tel: 212-983-9113
Fax: 212-983-9163
scott@bursor.com
jmarchese@bursor.com

Anthony Vozzolo (*pro hac vice*)
Christopher Marlborough (*pro hac vice*)
FARUQI & FARUQI, LLP
369 Lexington Ave., 10th Floor
New York, New York 10017
Tel: 212-983-9330
Fax: 212-983-9331
avozzolo@faruqilaw.com
cmarlborough@faruqilaw.com

Plaintiffs' Interim Class Counsel

Harry O. Channon (ARDC#6282644)
Mark D. Belongia (ARDC#6269391)
BELONGIA SHAPIRO & FRANKLIN LLP
20 South Clark Street, Suite 300
Chicago, Illinois 60603
Telephone: (312) 662-1030
Facsimile: (312) 662-1040
hchannon@belongialaw.com
mbelongia@belongialaw.com

William J. Doyle
DOYLE LOWTHER LLP
9466 Black Mountain Road, Suite 210
San Diego, California 92126
Telephone: (619) 573-1700
Facsimile: (619) 573-1701
bill@doylelowther.com

Katrina Carroll (ARDC#6291405)
LITE DEPALMA GREENBERG, LLC
One South Dearborn Street, Suite 1200

Chicago, Illinois 60603
Telephone: (312) 212-4383
Facsimile: (312) 212-5919
kcarroll@litedepalma.com

Joseph J. Siprut (ARDC#6279813)
SIPRUT PC
122 South Michigan Avenue, Suite 1850
Chicago, Illinois 60603
Telephone: (312) 588-1440
Facsimile: (312) 427-1850
jsiprut@siprut.com

Daniel A. Edelman (ARDC#00712094)
Cathleen M. Combs (ARDC#0047284)
James O. Latturner (ARDC#00472840)
Catherine A. Ceko (ARDC#6296053)
EDELMAN, COMBS, LATTURNER & GOODWIN, LLC
120 South LaSalle Street, 18th Floor
Chicago, Illinois 60603
Telephone: (312) 739-4200
Facsimile: (312) 419-0379
dedelman@edcombs.com
ccombs@edcombs.com
jlatturner@edcombs.com
cceko@edcombs.com

Additional Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I, Edmund S. Aronowitz, an attorney of record in this case, hereby certify that on September 9, 2011, the foregoing ***Plaintiffs' Memorandum of Law in Opposition to Defendant's Motion to Dismiss*** was filed electronically on the Court's CM/ECF system and thereby served electronically on the parties that have appeared in this action.

By: __/s/ Edmund S. Aronowitz___